

Network Scanning con Nmap

Josh Van Edward Abanico

7 gennaio 2026

Indice

1	Obiettivo dell'Esercitazione	2
2	Fase 1: Identificazione dei Target	2
2.1	Identificazione Target Linux (Metasploitable)	2
2.2	Identificazione Target Windows	3
3	Fase 2: Analisi Target Linux (192.168.10.4)	4
3.1	OS Fingerprinting	4
3.2	SYN Scan (Stealth Scan)	5
3.3	TCP Connect Scan e Confronto	6
3.3.1	Differenze Rilevate: SYN vs TCP Connect	6
3.4	Service Version Detection	7
4	Fase 3: Analisi Target Windows (192.168.10.5)	8
5	Conclusioni	8

1 Obiettivo dell'Esercitazione

L'obiettivo di questa attività è l'esecuzione di una scansione di rete approfondita su due target specifici all'interno del laboratorio virtuale:

1. **Target Linux:** Macchina *Metasploitable 2* (Vulnerabile by design).
2. **Target Windows:** Macchina *Windows 10*.

Sono state utilizzate diverse tecniche di scansione offerte dal tool **Nmap** per identificare sistemi operativi, porte aperte e versioni dei servizi, analizzando le differenze tra le metodologie TCP Connect e SYN Scan.

2 Fase 1: Identificazione dei Target

Prima di procedere con le scansioni esterne, è stata verificata la configurazione di rete locale delle macchine target per confermare gli indirizzi IP.

2.1 Identificazione Target Linux (Metasploitable)

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:b9:82:f3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.4/24 brd 192.168.10.255 scope global eth0
        inet6 fe80::a00:27ff:feb9:82f3/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Figura 1: Verifica IP Metasploitable (Command: ip a)

Indirizzo IP rilevato: 192.168.10.4

2.2 Identificazione Target Windows

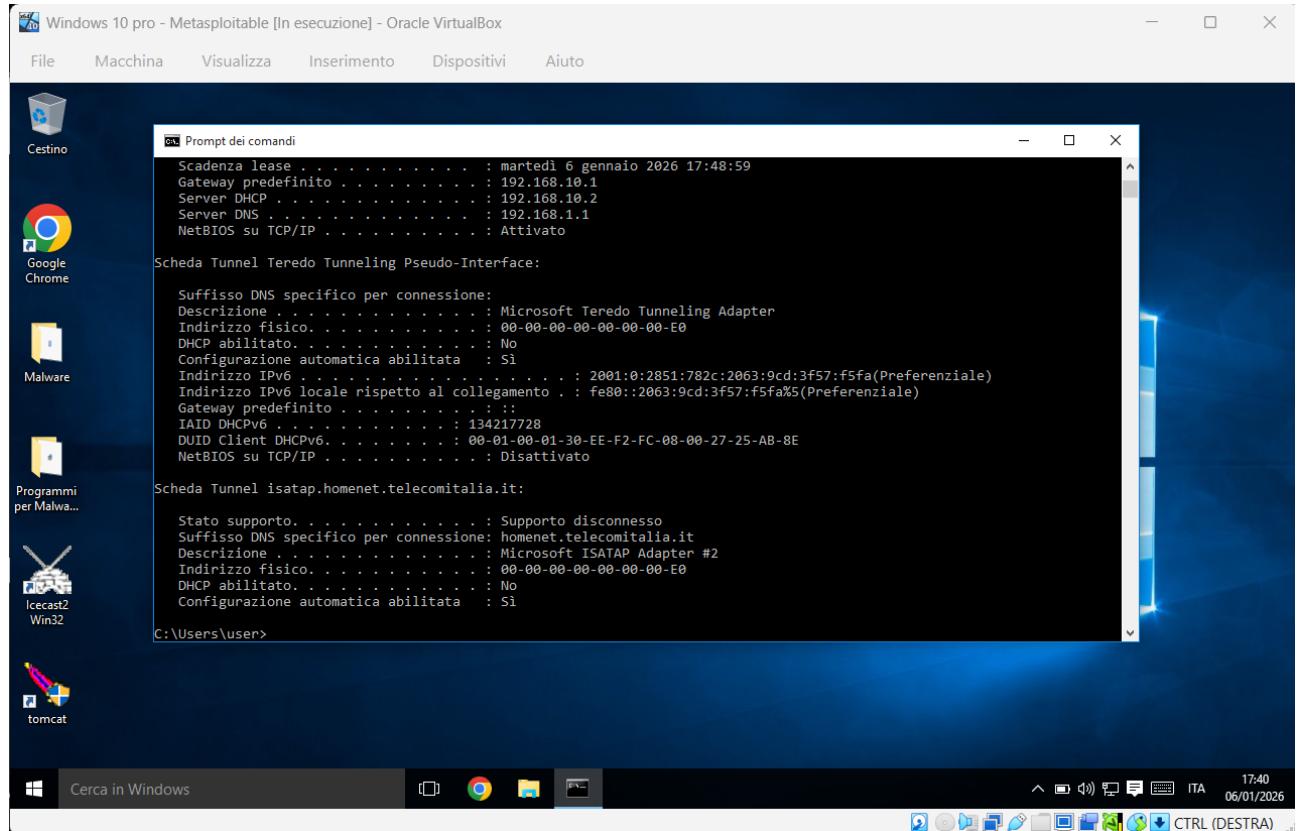


Figura 2: Verifica IP Windows (Command: ipconfig)

Indirizzo IP rilevato: 192.168.10.5

3 Fase 2: Analisi Target Linux (192.168.10.4)

3.1 OS Fingerprinting

È stata eseguita una scansione per identificare il Sistema Operativo sottostante.

```
sudo nmap -O 192.168.10.4
```

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:45 EST
Nmap scan report for 192.168.10.4 (192.168.10.4)
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:B9:82:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

Figura 3: Risultato OS Detection su Metasploitable

Il sistema è stato identificato come Linux, con un kernel compreso tra le versioni 2.6.9 e 2.6.33.

3.2 SYN Scan (Stealth Scan)

Scansione "half-open" eseguita con privilegi di root.

```
sudo nmap -sS 192.168.10.4
```

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:44 EST
Nmap scan report for 192.168.10.4 (192.168.10.4)
Host is up (0.00083s latency).

Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

MAC Address: 08:00:27:B9:82:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Figura 4: Risultato SYN Scan (-sS)

La scansione ha rilevato numerose porte aperte (es. 21, 22, 23, 25, 53, 80, 445, 3306) in tempi molto rapidi (0.27 secondi).

3.3 TCP Connect Scan e Confronto

Scansione completa del three-way handshake TCP.

```
sudo nmap -sT 192.168.10.4
```

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:44 EST
Nmap scan report for 192.168.10.4 (192.168.10.4)
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:B9:82:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Figura 5: Risultato TCP Connect Scan (-sT)

3.3.1 Differenze Rilevate: SYN vs TCP Connect

Dal confronto degli output (Fig. 4 e Fig. 5):

- **Risultati:** Entrambe le scansioni hanno rilevato le stesse porte aperte.
- **Performance:** La scansione SYN è risultata leggermente più performante in termini di stealth, non completando le connessioni.
- **Comportamento:** La scansione ‘-sT’ stabilisce una connessione completa (SYN → SYN-ACK → ACK), risultando più rumorosa nei log del target rispetto alla ‘-sS’ che invia un RST prima di stabilire la connessione.

3.4 Service Version Detection

Per enumerare le versioni specifiche dei servizi in ascolto.

```
sudo nmap -sV 192.168.10.4
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.10.4
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:26 EST
Nmap scan report for 192.168.10.4 (192.168.10.4)
Host is up (0.0024s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login        login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B9:82:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.82 seconds
```

Figura 6: Rilevamento versioni servizi (-sV)

Questa scansione è cruciale in quanto ha esposto versioni software potenzialmente vulnerabili (es. *vsftpd 2.3.4*).

4 Fase 3: Analisi Target Windows (192.168.10.5)

È stata effettuata una scansione combinata per rilevare il sistema operativo e le porte aperte sul secondo target.

```
sudo nmap -O 192.168.10.5
```

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:39 EST
Nmap scan report for 192.168.10.5 (192.168.10.5)
Host is up (0.0013s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
8443/tcp  open  https-alt
MAC Address: 08:00:27:25:AB:8E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (92%), Microsoft Windows Server 2008 R2
or Windows 7 SP1 (89%), Microsoft Windows 8.1 R1 (89%), Microsoft Windows Phone 7.5 or
8.0 (89%), Microsoft Windows Embedded Standard 7 (88%), Microsoft Windows 10 1511 - 1607
(87%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7
or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 10.41 seconds
```

Figura 7: Scansione OS e Porte su Windows

Il target presenta porte tipiche dell'ambiente Windows (135, 3389 RDP) ed è stato identificato con alta probabilità (92%) come Microsoft Windows 10.

5 Conclusioni

L'attività ha permesso di mappare con successo la superficie di attacco di entrambi i target. Mentre la macchina Windows presenta un numero limitato di servizi esposti (principalmente web e RDP), la macchina Linux (Metasploitable) espone un numero elevato di servizi con versioni obsolete (es. vsftpd 2.3.4, Apache 2.2.8).